

Noise powered amplification in CV quantum key distribution

Petr Marek and Radim Filip
*Department of Optics, Palacký University,
17. listopadu 1192/12, 771 46 Olomouc,
Czech Republic*

Amplification plays a key role in classical communication protocols, where it compensates the unavoidable loss of the signal. However, when we enter the quantum domain this approach starts being problematic as the standard kinds of amplifiers are usually accompanied by excess noise which detrimentally affects the quantum features of used states. Recently, several kinds of “noiseless” amplifiers that do not suffer from this feature have been proposed. Among these amplifiers, one that stands out is the noise powered amplifier, which acts incoherently, amplifying the signal by adding the “right” kind of noise. Here we show that despite the incoherence, which makes the amplifier unsuitable for protocols such as entanglement distillation, the added noise is not a big problem in quantum key distribution tasks and can be in some situations beneficial.

I. INTRODUCTION

Quantum physics poses hard fundamental limits on our ability to manipulate with information encoded into physical systems. One of these is the inability of extracting all of this ‘quantum information’ just from a measurement on a single copy of the quantum system, which is strongly related to the well known no-cloning theorem [1]. It is also the driving principle behind quantum key distribution (QKD) - the most developed application of quantum information theory yet. Continuous variable (CV) QKD [2] has recently appeared as an alternative to the initially developed protocols with single photons. It utilizes coherent and squeezed states of light, relying on homodyne instead of single photon detectors. In the absence of noise it principally allows for secure communication over arbitrarily lossy channel [3]. In reality, though, certain amount of noise is unavoidable and loss is therefore the chief factor in limiting the communication distance.

In classical communication protocols it is customary to compensate the loss with help of amplifiers - an approach which not possible in the quantum domain, as the existing phase insensitive amplifiers add enough noise to the system to render whole procedure counterproductive [4]. In fact, the ideal noiseless amplifier, which would be able to fully compensate the loss at least at some level by allowing coherent states to be transformed as $|\alpha\rangle \rightarrow |g\alpha\rangle$, is represented by an unbounded trace increasing operator and therefore does not exist as a physical operation.

However, it is possible to devise an approximation of the amplification device. There have been several proposals with varying levels of technological sophistication, ranging from proposals based on quantum scissors [5], over additions and subtractions of individual photons [6–8], up to deliberate injection of noise followed by photon subtractions [6, 9]. The last mentioned kind of amplifier is different from the others - it utilizes a noise addition as part of the process. Noise addition, which is exactly the opposite of that what we are trying achieve. This is not without repercussions, as this type of amplifier is, unlike

the others, incoherent. It reduces purity of the state and, when applied to entangled state, reduces entanglement as well. Interestingly enough, quantum communication is not only about entanglement and in this paper we show, there are regimes in which this apparently less-than-ideal amplifier outperforms its more effective counterparts.

Recently there have been several studies related to application of amplifiers in communication tasks. In [10] it was shown that the amplifier based on quantum scissors can be used for compensation of losses and distillation of entanglement. A related issue was discussed in [11, 12], where it was shown that Gaussian data processing virtually simulating the effect of the ideal amplifier can be used to enhance the rate of secure key distribution in CV QKD.

In this paper we look closely at two kinds of noiseless amplifiers and analyze how beneficial they can be when used in communication protocols. In Sec. II we introduce the formal description of the communication protocol and of the amplifiers. In Sec III we analyze the amplifiers for use in communication over ideal channels. In sec. IV we expand the treatment by considering realistic channels with loss and noise. The results are finally summarized in sec. V.

II. COMMUNICATION PROTOCOL AND AMPLIFICATION

The secure key distribution between Alice and Bob, which is schematically depicted in Fig. 1, can be always represented by an entangled two-mode quantum state, which is shared and locally measured by the two communicating parties. Entanglement is a necessary part of the state, without it the shared correlations are inherently classical and no secure key can be established. In a continuous variables CV quantum key distribution, the shared quantum state is a two mode squeezed state and the measurements performed can be either of the homodyne, or of the heterodyne variety. The measurement at Alice’s side determines the nature of the communication: homodyne or heterodyne measurement represents

communication with squeezed or coherent states, respectively. Measurement at Bob's side bears no such significance.

There are several factors deciding the amount of information which can be transmitted in this way: the shared quantum state and the measurements performed on its two parts. For two sets of measurements, A and B , with possible measurement outcomes $\{a\}$ and $\{b\}$, respectively, the amount of mutual information shared by Alice and Bob after a single round of measurements on quantum state ρ is given by:

$$I(A, B) = \int p(a, b) \log_2 \frac{p(a, b)}{p(a)p(b)} da db, \quad (1)$$

where $p(a, b) = \text{Tr}[\rho \Pi_a \otimes \Pi_b]$ is a joint probability distribution of Alice measuring value a and Bob measuring value b , where these events are represented by the projectors Π_a and Π_b . $p(a)$ and $p(b)$ are then marginal probability distributions of the individual measurements. For our analysis we consider two possible classes of measurements, which have been previously applied to CV quantum communication. Homodyne measurement returns single real values x , each of which corresponds to one particular projector on a specific x quadrature eigenstate $|x\rangle\langle x|$. Heterodyne measurement consists of two homodyne measurements measuring in two conjugated bases, as such it results in a pair of values x and p , with corresponding projector $\Pi_{x,p} = |\alpha\rangle\langle\alpha|$, where $|\alpha\rangle$ is a coherent state with amplitude $\alpha = (x + ip)/\sqrt{2}$. In principle, any non-factorable quantum state shared between Alice and Bob can be used for communication. Practical CV communication protocols employ exclusively Gaussian states, fully described by their variance matrix, for which the formulas can be simplified significantly [3].

In the ideal scenario, the shared quantum state ρ is pure and the amount of mutual information is given by its entanglement. This ceases to be the case in the presence of channel loss and noise. However, their influence only transforms the density matrix of the shared state and the methodology for obtaining the amount of information transferrable remains unchanged. The same goes for any kind of probabilistic operation applied to the quantum state. In the following we shall be mostly concerned with various kinds of noiseless amplification, which aims at increasing the mutual information at the cost of reduced probability of success. Operations of these kind can be always represented by trace decreasing maps \mathcal{A} and the amplified state is then

$$\rho_{amp} = \frac{\mathcal{A}(\rho)}{\text{Tr}[\mathcal{A}(\rho)]}. \quad (2)$$

Ideal noiseless amplification is represented by operator $G = g^n$, where n is the photon number operator, and it transforms an arbitrary coherent state into $G|\alpha\rangle = |g\alpha\rangle$. The operation is easy to work with and it has the added benefit of being Gaussian - it preserves the Gaussian nature of Gaussian states, which are the staple of contem-

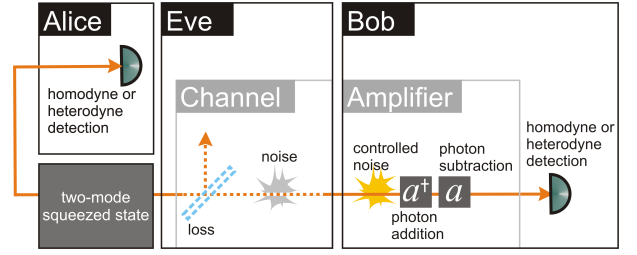


FIG. 1: (Color online) Schematic setup of the communication protocol.

porary communication protocols. However, since the operator is unbounded for $g > 1$, it does not represent a physical operation and in its exact form it can not be experimentally implemented. When one is interested in amplification of weak states, though, the amplification can be approximatively implemented in several ways [4]. It should be stressed that all these realistic amplification procedures are not Gaussian, one can therefore no longer rely just on the description by variance matrix and needs to employ the density matrix to obtain the mutual information (1).

In the following, we shall focus on amplifiers employing the photon-addition and photon-subtraction operations [6, 7], performance of which has been experimentally verified for coherent states with reasonably large amplitudes [8, 9]. The two amplifiers are the 'High-Fidelity amplifier' (HFA) and the 'Noise-powered amplifier' (NPA). The first one can be implemented by adding-and-then-subtracting a number of photons, while the second one replaces the photon addition step by deliberate addition of thermal noise. As a consequence, HFA preserves purity of the amplified quantum state and can be, in principle, employed for entanglement distillation, while NPA can not. On the other hand, NPA is much less experimentally demanding significantly higher numbers of subtracted photons can be achieved.

We can devise a general form fusing HFA and NPA together. Such the amplifier is obtained by the sequence of noise addition, photon addition, and photon subtraction, and it transforms an arbitrary quantum state ρ to

$$\frac{1}{\mathcal{N}} a^N a^{\dagger M} \left[\int \frac{e^{-|\alpha|^2/\Delta}}{\pi\Delta} D(\alpha) \rho D^\dagger(\alpha) d^2\alpha \right] a^M a^{\dagger N}, \quad (3)$$

where \mathcal{N} is a normalization factor assuring unit trace of the resulting density matrix. The amplifier is quantified by three parameters - the amount of added noise Δ and the numbers of photons added, M , and subtracted N . HFA and NPA are now obtained by setting $\Delta = 0$ and $M = 0$, respectively.

III. IDEAL SCENARIO

Let us first analyze the ideal scenario, in which the channel is perfect - there is no loss or noise present in

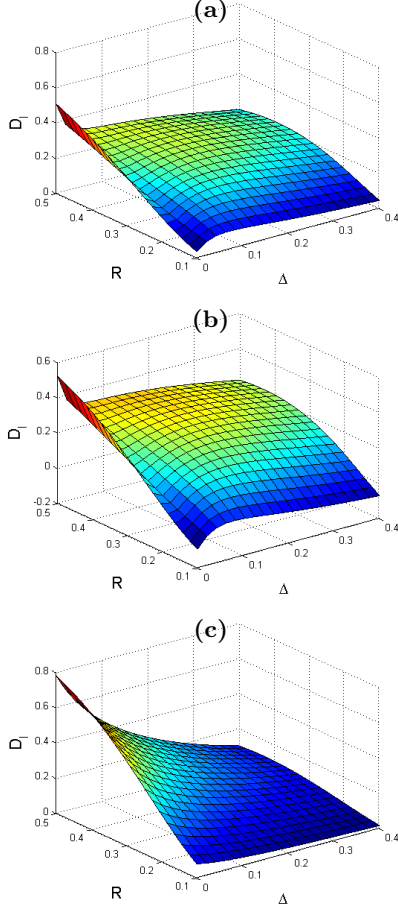


FIG. 2: (Color online) Difference of mutual information for two-photon subtraction (a), three photon subtractions (b), and addition and subtraction of a photon (c), in relation to the squeezing of the initial state R and the amount of noise added prior to the operations Δ . Both Alice and Bob perform homodyne detection.

it. This corresponds to situation in Fig. 1 only with Eve completely removed from the picture. In this case the mutual information is solely given by the entanglement of the initial two-mode squeezed state, which is a Gaussian state fully described by its variance matrix

$$V = \frac{1}{2} \begin{pmatrix} \cosh 2R & 0 & \sinh 2R & 0 \\ 0 & \cosh 2R & 0 & -\sinh 2R \\ \sinh 2R & 0 & \cosh 2R & 0 \\ 0 & -\sinh 2R & 0 & \cosh 2R \end{pmatrix}, \quad (4)$$

where R is the squeezing parameter. In Fock representation, the density matrix of the state can be expressed as

$$\rho = \frac{1}{\cosh 2R} \sum (\tanh 2R)^{n+m} |n, n\rangle \langle m, m|. \quad (5)$$

From here we can directly obtain the amplified form of state by using (3), and then use this new amplified state to obtain new mutual information shared by the communicating parties. We can then plot the difference of

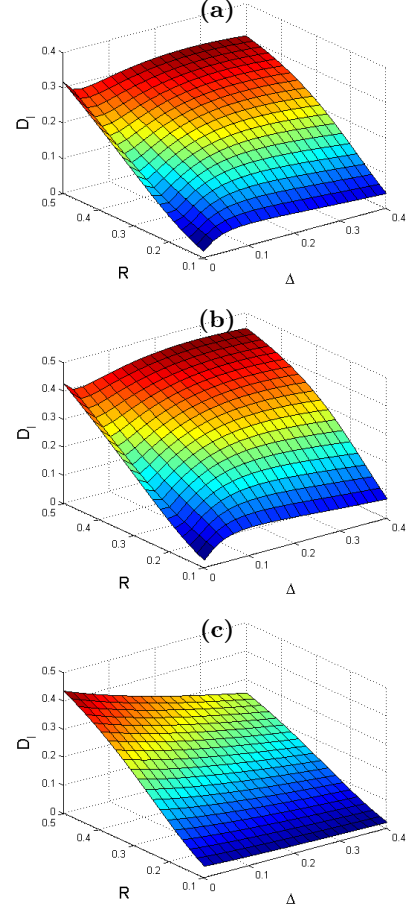


FIG. 3: (Color online) Difference of mutual information for two-photon subtraction (a), three photon subtractions (b), and addition and subtraction of a photon (c), in relation to the squeezing of the initial state R and the amount of noise added prior to the operations Δ . Alice and Bob perform homodyne and heterodyne detections, respectively.

mutual information before and after the amplification, $D_I = I(A, B) - I_0(A, B)$ in dependence on the parameters of the communication. One of these parameters is the squeezing parameter R representing the communication, the other is the amount of noise added in the amplification step Δ .

The three specific amplification configurations we are going to compare are: addition of noise and subtraction of two photons, addition of noise and subtraction of three photons, and addition of noise followed by addition and then subtraction of a photon. The first two are essentially the same device, differing only by the number of subtractions, which is responsible for strength of the operation. The third one is a hybrid of the pure HFA and NPA. Values for the ideal HFA are easily obtained by looking at the edge of the graph, but the full picture will be useful in determining whether there are any benefits to adding noise.

In Fig. 2 we see the difference in mutual information

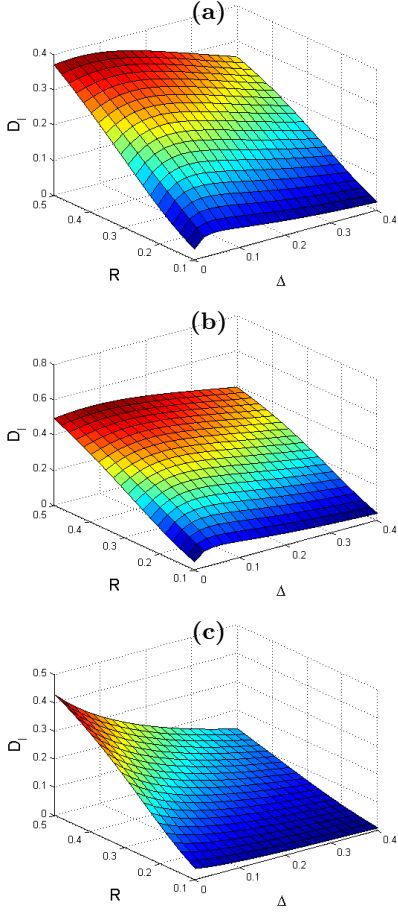


FIG. 4: (Color online) Difference of mutual information for two-photon subtraction (a), three photon subtractions (b), and addition and subtraction of a photon (c), in relation to the squeezing of the initial state R and the amount of noise added prior to the operations Δ . Alice and Bob perform heterodyne and homodyne detections, respectively.

when both Alice and Bob perform homodyne detections. This corresponds to direct communication, in which Alice encodes information into a displaced squeezed state and Bob measures the displacement by homodyne detection. We can see that all three nonclassical operations we have considered, two photon subtraction in Fig. 2a, three photon subtraction in Fig. 2b, and photon addition and subtraction in Fig. 2c, increase the mutual information when no noise is present, with the last one of the three providing the largest benefit. In this scenario, the effect of added noise is almost completely detrimental. The exception are the photon subtraction schemes, where a larger amount of noise is usually better than a small one (even though no noise is the best, unless the shared entanglement is very small).

The situation starts being different when Bob uses heterodyne measurement instead of the homodyne one, while Alice keeps using homodyne detection (encoding into squeezed states), which is the situation represented

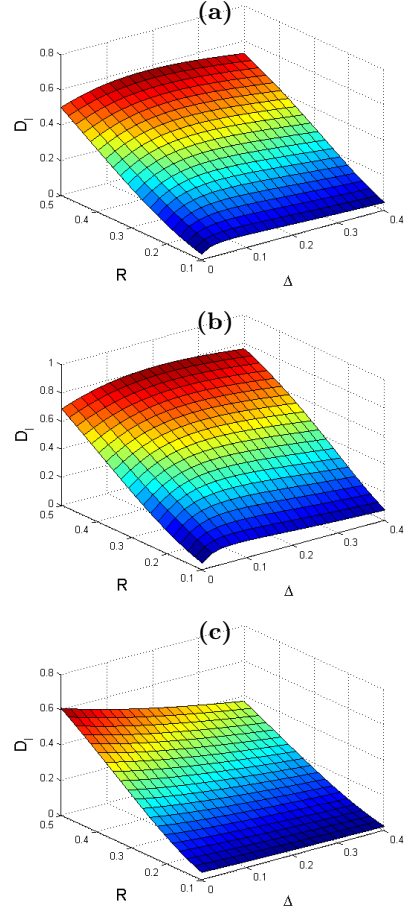


FIG. 5: (Color online) Difference of mutual information for two-photon subtraction (a), three photon subtractions (b), and addition and subtraction of a photon (c), in relation to the squeezing of the initial state R and the amount of noise added prior to the operations Δ . Both Alice and Bob perform heterodyne detections.

by Fig. 3. This is slightly similar to a situation in CV QKD, where the seemingly suboptimal measurement on the Bob's side allows for increasing secure communication distance by reducing information gained by eavesdropper Eve [14]. In this scenario all the employed non-Gaussian operations lead to improvement of mutual information. And again, when only photon subtractions are used, addition of noise can improve the information gain even further. And this can be said for all regimes, in which coherent states are employed. Next to the squeezed-heterodyne protocol, which was just mentioned, there is the encoding into coherent states, which are measured either by homodyne, or by heterodyne detection. This scenarios are represented by Fig. 4 and Fig. 5.

In summary we can say that, when communicating solely with squeezed states and homodyne detection, the non-gaussian operations lead to improvement, which is generally not helped by inclusion of additional noise. However, as soon as coherent states start being employed,

either at the state preparation or at the measurement stage, the situation changes. While photon addition and subtraction still works best without any noise present, photon subtraction schemes are further enhanced by it. It can be even said that the noise compensates the advantage photon addition has over photon subtraction. On the level of mutual information, addition and subtraction of photon is observably better than subtraction of two photons and roughly on the level of three photon subtractions. With added noise, two subtractions can match the addition and subtraction, and three subtractions overcome it significantly.

IV. REALISTIC CHANNEL

So far we have only considered the ideal case, in which the communication channels suffers from no losses or noise. This is an artificial scenario far removed from practical conditions. It's results give us some insight into the benefits of the amplification, but it is not enough. The biggest concern related to the loss and noise is not about how information between Alice and Bob gets lost, but how it leaks out towards the third party - the nefarious eavesdropper Eve. Increasing mutual information of Alice and Bob is of no use, if the information Gained by Eve is raised by the same, or higher, amount. We shall not restrict Eve to using a specific type of eavesdropping interaction or measurements. In our treatment by effective entanglement, we can represent the communication by a three-mode entangled state ρ_{ABE} such that $\rho_{AB} = \text{Tr}_E[\rho_{ABE}]$ is equivalent to a density matrix of a two-mode squeezed state for which one of the modes is affected by loss η and noise N_T . As a consequence, ρ_{AB} represents a Gaussian state with variance matrix

$$V_{AB} = \Xi V \Xi + (1 - \Xi^2) N_T, \quad (6)$$

where $\Xi = \text{diag}[(1, 1, \sqrt{\eta}, \sqrt{\eta})]$ and V is taken from (4). However, the global state ρ_{ABE} is pure - all the noise and loss present in the state, which is shared by Alice and Bob, represents information gained by Eve. After Bob performs his measurement, obtaining value b with probability $P(b)$ and leaving the Alice's and Eve's modes in the state $\rho_{AE}(b)$, the information about Alice's initial state gained by Eve can be upper-bounded by Holevo quantity [16]:

$$\begin{aligned} H(E; A) &= S(\rho_E) - \int P(b) S[\rho_E(b)] db \\ &= S(\rho_{AB}) - \int P(b) S[\rho_A(b)] db. \end{aligned} \quad (7)$$

Here $S(\cdot)$ stands for von Neumann entropy, $\rho_E = \text{Tr}_{AB}[\rho_{ABE}]$, $\rho_E(b) = \text{Tr}_A[\rho_{AE}(b)]$, $\rho_A(b) = \text{Tr}_E[\rho_{AE}(b)]$, and we have taken advantage of purity of ρ_{ABE} and $\rho_{AE}(b)$. For the case of reverse reconciliation, where Eve's knowledge about Bob's measurement result is given

by $H(E; B)$, similar relation can be obtained by interchanging variables corresponding to Alice and Bob,

$$\begin{aligned} H(E; B) &= S(\rho_E) - \int P(a) S[\rho_E(a)] da \\ &= S(\rho_{AB}) - \int P(a) S[\rho_B(a)] da, \end{aligned} \quad (8)$$

where $\rho_E(a) = \text{Tr}_B[\rho_{BE}(a)]$, $\rho_B(a) = \text{Tr}_E[\rho_{BE}(a)]$, and $\rho_{BE}(a)$ represents the state of the system after Alice's measurement yielded value a with probability $P(a)$.

The purity of the global state is an important assumption, which does not mesh well with the noise-powered amplification routine. If the amplification noise was simply added, it would lead to overestimation of Eve's information. Therefore, we are going to represent the noise addition in a different manner. Taking hints from the virtual entanglement approach, we introduce an ancillary state $|\nu\rangle = \sum_{k=0}^8 c_k |k\rangle$ to which corresponds a set of coherent amplitudes β_k such that $\beta_0 = 0$ and $\beta_k = \sqrt{\Delta'} e^{i2k\pi/8}$. The coefficients c_k can be arbitrary, but we have chosen $c_0 = 1$ and $c_k = e^{-\Delta'/2}$ for $k = 1, \dots, 8$ (prior to normalization) to emulate Gaussian distribution of thermal noise. This state is under Bob's control and the process of noise addition can be now described by

$$\rho \rightarrow \sum_{k=0}^8 D(\beta_k) \otimes |k\rangle\langle k| (\rho \otimes |\nu\rangle\langle\nu|) \sum_{k=0}^8 D(-\beta_k) \otimes |k\rangle\langle k|. \quad (9)$$

For the purpose of obtaining the mutual information between Alice and Bob, the ancillary mode ν is traced over. For the purpose of obtaining Eve's information, Bob is considered measuring both modes B and ν . The noise modeled in this way is non-Gaussian, but because we consider the noise addition procedure to be under our control, there are no limits to the actual form the noise might take. In fact, it was even demonstrated that non-Gaussian noise is beneficial for some kinds of applications [15].

The analysis has been again performed for a single quantum state (two mode squeezed state with $R = 0.3$) used in four different communication protocols represented by combinations of measurements Alice and Bob can perform. Table III shows the differences of the relative quantities before the operation and after. Positive and negative values correspond to the values being increased and decreased, respectively, by the amplification operation.

The benefits of amplification are best visible in scenarios in which Alice and Bob's measurements match - they both perform either homodyne (squeezed state communication), or heterodyne (coherent states communication) detections. The number of scenarios is doubled, though, by considering both direct and reverse reconciliation. The further analysis shall be therefore concerned only with those scenarios. Four different Gaussian channels have been analyzed and the results can be seen in Table III.

	Δ'	Two photon subtraction					
		Homodyne - Homodyne			Heterodyne - Heterodyne		
		$I(A,B)$	$H(E;A)$	$H(E;B)$	$I(A,B)$	$H(E;A)$	$H(E;B)$
$\eta = 1, N_T = 0$	0	0.2988	0	0	0.1870	0	0
	0.1	0.2796	0	0	0.3011	0	0
	0.2	0.3299	0	0	0.3411	0	0
	0.3	0.3530	0	0	0.3554	0	0
$\eta = 1, N_T = 0.1$	0	0.3093	0.8499	-0.1927	0.3234	1.0678	-0.3218
	0.1	0.3322	0.3087	-0.1756	0.3398	0.4134	-0.2044
	0.2	0.3322	0.4295	-0.1949	0.3369	0.5798	-0.2662
	0.3	0.3217	0.2337	-0.1710	0.3272	0.3101	-0.1651
$\eta = 0.9, N_T = 0$	0	0.2635	0.0631	0.0209	0.1708	0.1083	0.0256
	0.1	0.2706	0.0184	0.0181	0.2846	0.0628	0.0247
	0.2	0.3209	0.0107	0.0161	0.3229	0.0470	0.0233
	0.3	0.3429	0.0066	0.0144	0.3359	0.0380	0.0220
$\eta = 0.9, N_T = 0.1$	0	0.2994	0.9805	0.2630	0.3060	1.2143	0.3375
	0.1	0.3207	0.4356	0.2783	0.3202	0.5624	0.4527
	0.2	0.3191	0.5544	0.2553	0.3164	0.7242	0.3871
	0.3	0.3078	0.3621	0.2856	0.3065	0.4626	0.4955
	Δ'	Photon addition and subtraction					
		Homodyne - Homodyne			Heterodyne - Heterodyne		
		$I(A,B)$	$H(E;A)$	$H(E;B)$	$I(A,B)$	$H(E;A)$	$H(E;B)$
$\eta = 1, N_T = 0$	0	0.5038	0	0	0.2886	0	0
	0.1	0.3176	0	0	0.2456	0	0
	0.2	0.2378	0	0	0.2166	0	0
	0.3	0.1904	0	0	0.1939	0	0
$\eta = 1, N_T = 0.1$	0	0.3292	0	0	0.2476	0	0
	0.1	0.2431	-0.0153	-0.1868	0.2143	-0.0195	-0.1039
	0.2	0.1934	-0.0266	-0.2695	0.1897	-0.0339	-0.1625
	0.3	0.1592	-0.0355	-0.3191	0.1699	-0.0453	-0.2057
$\eta = 0.9, N_T = 0$	0	0.4674	-0.0009	0.0099	0.2664	0.0135	0.0131
	0.1	0.2950	-0.0010	0.0072	0.2262	0.0120	0.0114
	0.2	0.2210	-0.0011	0.0057	0.1993	0.0110	0.0103
	0.3	0.1774	-0.0012	0.0049	0.1784	0.0102	0.0094
$\eta = 0.9, N_T = 0.1$	0	0.3045	0.1353	0.4833	0.2278	0.1662	0.6682
	0.1	0.2250	0.1207	0.2760	0.1969	0.1478	0.5604
	0.2	0.1793	0.1100	0.1890	0.1742	0.1341	0.5014
	0.3	0.1478	0.1015	0.1378	0.1559	0.1235	0.4582

TABLE I: Comparison of differences in mutual information between Alice and Bob, $I(A, B)$, and differences Holevo quantities for the eavesdropper Eve for both direct and reverse reconciliation, $H(E; A)$ and $H(E; B)$, respectively. The values are compared across two kinds of amplification operations with several levels of added noise, two communication protocols characterized by measurements performed by Alice and Bob, and four different channels represented by their loss η and added noise N_T . See the main text for more details.

The first channel is again the ideal one, with no losses or added thermal noise. In such the channel Eve has no information and this remains unchanged under amplification, which still does increase the mutual information between Alice and Bob, as was discussed in section III. The second type of channel is represented by added noise of $N_T = 0.1$ but no loss. In this case, both amplifiers across all the four communication protocols improve Alice's and Bob's situation over Eve's. It is interesting now, to look at the effect of added noise. For two photon subtraction, adding noise both improves $I(A, B)$ and (most

of the time) reduces $H(E; \cdot)$. As a consequence, noise is necessary if the amplification is to have positive impact for direct reconciliation protocols. For addition and subtraction of a photon, the noise does not improve $I(A, B)$ at all, as could be expected from the analysis of the pure case. However, the noise hampers Eve even more - so much, in fact, that for reverse reconciliation protocols it is significantly more beneficial than the pure scenario.

The third channel is pure lossy channel with $\eta = 0.9$, with no thermal noise. As such, it is very similar to the ideal noiseless and lossless channel in it's capacity to

accommodate amplifiers - both of them lead to improvements for all communication protocols, with artificial addition of noise being useful for two photon subtraction and detrimental for photon addition and subtraction.

The last considered channel exhibits both noise $N_T = 0.1$ and loss $\eta = 0.9$. As such it is the scenario with strongest ties to reality. What distinguishes it from the other scenarios most, is the comparatively huge improvement in information Eve gains when Alice and Bob attempt any amplification. It is so significant, in fact, that for communication via coherent states (heterodyne-heterodyne) the NP amplifier fails to achieve any improvement. It can, however, be helpful in the case squeezed state communication (homodyne-homodyne) with reverse reconciliation. In this case, the artificially added noise is not necessary, but helpful. On the other hand, the HF amplifier is helpful only for the direct reconciliation protocol and for those the addition of noise is only detrimental. Interestingly enough, when enough noise is added, addition and subtraction of photon can also lead to improvement for reverse reconciliation in the squeezed state communication.

Let us pause now and attempt to summarize the effect of artificial added noise. If addition of noise precedes two photon subtraction, it generally increases mutual information between Alice and Bob. However, at the same time it also increases (for reverse reconciliation) or decreases (for direct reconciliation) the information of Eve. On the other hand, for addition and subtraction of photon, addition of noise always hurts Alice and Bob, but it also always reduces the influence of Eve. As a consequence, for both types of amplifier there are scenarios, when addition of noise is beneficial, and even scenarios, when is it essential for improvement to appear.

V. SUMMARY

We have analyzed the effect noiseless amplifiers can have on quantum communication. Specifically we were concerned with two types of amplifier: HF amplifier consisting of photon addition and subtraction, and NP amplifier realized by addition of noise and photon subtraction.

Special attention was devoted to the effect of artificial noise addition - its influence was also studied for the HF amplifier, even though the original design does not call for it.

First we have studied the amplifiers purely from the perspective of mutual information between the communicating parties. It was revealed, that both amplifiers can improve the mutual information. The effect of artificial noise differs, though. For the HF amplifier the noise is always detrimental. For the NP amplifier, however, it improves the situation almost to the level of the HF amplifier - addition and subtraction of photon is significantly better than two photon subtraction (hinting towards photon addition being more ‘powerful’ operation than photon subtraction), but roughly at the same level as two photon subtraction after noise addition.

In the second step we have analyzed the amplifiers within the context of a full communication protocol, with eavesdropper Eve included. To have comparison between several physical scenarios, we have studied four different quantum channels: ideal channel, purely noisy channel, purely lossy channel, and realistic noisy and lossy channel. For channels without any added noise, both amplifiers work reliably and without surprises - the performance is mostly given by changes in mutual information, which is increased by the amplification for all communication scenarios. For the purely noisy channel, both amplifiers lead to improvement, but surprisingly, even the performance of the HF amplifier can be improved by adding artificial noise. If the channel is lossy and noisy at the same time, the regimes in which the amplifier is beneficial are most difficult to find, but it can be done. And again, it may be advantageous, for both types of amplifiers, to add a measure of artificial noise.

We have shown that realistic experimentally feasible amplifiers can be used to improve existing quantum information protocols, and that addition of artificial noise can play an important role in this task.

Acknowledgments We acknowledge support from grant P205/12/0577 of Grant Agency of Czech Republic.

-
- [1] W. Wothers and W. Zurek, *Nature* 299, 802 (1982).
 - [2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, *Rev. Mod. Phys.* 81, 1301 (2009).
 - [3] F. Grosshans, G. Van Assche, J. Wenger R. Brouri, N. J. Cerf, and P. Grangier, *Nature* 421, 238 (2003).
 - [4] C. M. Caves, *Phys. Rev. D* 26, 1817-1839 (1982).
 - [5] T. C. Ralph and A. B. Lund, in *Proceedings of the Ninth International Conference on Quantum Communications Measurement and Computing*, edited by A. Lvovsky, AIP Conf. Proc. No. 155 (AIP, New York, 2009); G. Y. Xiang, T. C. Ralph, A. P. Lund, N. Walk, and G. J. Pryde, *Nat. Photon.* 4, 316 (2010); F. Ferreyrol, M. Barbieri, R. Blandino, S. Fossier, R. Tualle-Brouri, and P. Grangier, *Phys. Rev. Lett.* 104, 123603 (2010)
 - [6] P. Marek and R. Filip, *Phys. Rev. A* 81,
 - [7] *Phys. Rev. A* 81, 022302 (2010); J. Fiurasek, *ibid.* 80, 053822 (2009).
 - [8] A. Zavatta, J. Fiurasek, and M. Bellini, *Nat. Photon.* 5, 52 (2011);
 - [9] M. A. Usuga, C. R. Muller, C. Wittmann, P. Marek, R. Filip, C. Marquardt, G. Leuchs, and U. L. Andersen, *Nat. Phys.* 6, 767 (2010).
 - [10] T.C.Ralph, *Phys. Rev. A* 84, 022339 (2011).

- [11] J. Fiurášek and N. J. Cerf, arXiv quant-ph (2012)
- [12] Nathan Walk, Thomas Symul, Ping Koy Lam, Timothy C. Ralph, arXiv:1206.0936
- [13] T. C. Ralph, Phys. Rev. A 84, 022339 (2011).
- [14] R. García-Patrón and N. J. Cerf, Phys. Rev. Lett. 102, 130501 (2009).
- [15] C. R. Muller, C. Wittmann, P. Marek, R. Filip, C. Marquardt, G. Leuchs, and U. L. Andersen, Phys. Rev. A 86, 010305(R) (2012).
- [16] M.A. Nielsen and I.L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, (2000).